电子商务概论知识辅导：加密技术 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/170/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_170733.htm 迄今为止，对网络和通信安全的最重要的自动工具是加密，电子商务中通常使用两种形式的加密：常规加密和公钥加密。一、基本概念1、明文：可理解的信息，即原始信息。2、 密文：经过转换，表面上看来是无规则、无意义的信息。3、 加密技术：是实现信息保密性的一种重要的手段，目的是为了防止合法接收者之外的人获取信息系统中的机密信息。二、 密钥密钥图6.6 加密解密过程明文 加密运算 密文 解密运算 明文加密过程：加密过程由算法和密钥构成。2、密钥：密钥是控制算法并独立于明文的值，同算法一起加密明文。密钥分为加密密钥、解密密钥。三、密码学围绕加密和解密过程就出现了两门学科：密码编码学和密码分析学。这两门学科合起来就称为密码学。1、密码编码学：密码编码学主要研究对数据进行变幻的原理、手段和方法，主要进行密码体制设计，目的是为了设计出安全的密码体制。2、密码分析学：密码分析学进行密码分析，在未知密钥的情况下，从密文推出明文或密钥的技术，是用来研究如何破译密文的。密码编码学和密码分析学这两门学科尽管表面看来相互对立，但在整个密码学的发展中，却是相辅相成、互相促进的。四、加密体制：按照加密密钥和解密密钥是否相同，可将现有的加密体制分为：单钥加密体制和双钥加密体制。1、单钥加密体制单钥加密体制又称为私钥或对称加密体制。这种体制的加密密钥和解密密钥相同或者本质上相同（即从其中一个可以很容易地推出另一

个）。2、双钥加密体制 双钥加密体制又称公钥（或非对称）加密体制。这种体制的加密密钥和解密密钥不相同，而且从其中一个很难推出另一个。这样加密密钥可以公开，而解密密钥可由用户自已秘密保存。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com